概论

2020年3月31日 21:33

1. 信息安全
    a. 计算机安全
        i. 目标：包括保护信息免受未经授权的访问、中断和修改，同时为系统的预期用户保持系统的可用性
        ii. 定义：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露
    b. 网络安全
        i. 研究对象：整个网络，研究领域比计算机系统安全更为广泛
        ii. 目标：要创造一个能够保证整个网络安全的环境，包括网络内的计算机资源、网络中传输及存储的数据和计算机用户。通过采用各种技术和管理措施，使网络系统正常运行，确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等
        iii. 涉及的领域：密码学设计，各种网络协议的通信以及各种安全实践等
    c. 信息安全

        定义：信息安全是为防止意外事故和恶意攻击而对信息基础设施、应用服务和信息内容的保密性、完整性、可用性、可控性和不可否认性进行的安全保护

        目的：信息安全作为一个更大的研究领域，对应信息化的发展，信息安全包含了信息环境、信息网络和通信基础设施、媒体、数据、信息内容、信息应用等多个方面的安全需要
2. 发展史
    a. 古典信息安全
        i. 物理性安全措施，Caesar密码，语音加密(纳瓦霍语)，one-pad-time
    b. 辐射安全
        i. 搜集电磁辐射，还原信息
    c. 计算机安全
    d. 网络安全
        i. 无线网络安全
    e. 信息安全
3. 信息安全面临的挑战
    a. 互联网体系结构的开放性
    b. 网络基础设施和通信协议的缺陷
    c. 网络应用高速发展
    d. 黑客
    e. 恶意软件
    f. 操作系统漏洞

g. 内部安全
h. 社会工程学

4. 攻击与威胁
    a. 威胁：破坏安全的潜在可能，在环境、能力、行为或事件允许的情况下，它们会破坏安全，造成危害；
    b. 攻击：对系统安全的攻击，它来源于一种具有智能的威胁，也就是说，有意违反安全服务和侵犯系统安全策略的智能行为；
        i. 被动攻击：试图理解或利用系统的信息但不影响系统资源；对传输进行窃听和监测
        ii. 主动攻击：试图改变系统资源或影响系统运作；对数据流进行修改或伪造数据流
    c. 区别：
        i. 可能导致破坏发生的行为被称为攻击(attack)
        ii. 破坏行为的完成者被称为攻击者
5. 攻击
    a. 被动攻击passive attack
        i. 重点是预防，而不是检测
        ii. 通过加密可解决
    b. 主动攻击active attack
        i. 难以绝对预防，但容易检测
        ii. 包括：伪装、重播、消息修改、拒绝服务
    c. 其他攻击
        i. 信源否认：即某实体欺骗性地否认曾发送（或创建）某些信息，是某种形式的欺骗。
        ii. 信宿否认：某实体欺骗性地否认曾接收过某些信息或消息，也是一种欺骗。
        iii. 延迟：暂时性地阻止某种服务，这是一种篡夺攻击，尽管它能对欺骗起到支持的作用。
6. 信息安全五性（前三项CIA三元组体现了数据、信息、计算机服务的基本安全目标）
    a. 保密性confidentiality：确保信息不会被泄漏给嗅探者，常通过用加密算法和密钥对信息进行加密实现
    b. 完整性integrity：保护数据免受非授权的修改，常通过hash算法制作摘要实现
    c. 可用性availability：保证资源能被用户合理使用，常通过登陆用户验证和CDN等方法实现；
    d. 可控性controllability：能标识资源，如验证用户的身份，常通过密码或生物特征实现；
    e. 不可否认性non-repudiation：保证信息源头可辨认，常通过信息发布者的数字签名实现。
7. 安全：避免由于任何风险、危险和威胁所能带来的伤害的能力，是不可能达到的
    a. 恰当的安全：保护机构的财产和利益，这建立在对财产和利益的风险预期（Risk Appetite）和风险容忍（Risk Tolerance）

i. 风险预期：通过采取措施必须控制降低的风险部分
ii. 风险容忍：其余的风险，可接受的部分

b. 安全性分类
i. 无条件安全性：$I(X;Y)=H(X)-H(X\mid Y)=0$
ii. 计算上的安全性：计算资源受限
iii. 复杂度理论的安全性：计算上是困难
iv. 可证明的安全性：规约为数学问题
v. 非密码的、系统的安全性：不期望的状态不可达

8. 信息安全风险分析
a. 信息资产：物理资产、知识资产、时间资产和名誉资产
b. 信息安全评估：
i. 安全漏洞：安全漏洞即存在于系统之中，可以用于越过系统的安全防护
ii. 安全威胁：安全威胁是一系列可能被利用的漏洞
iii. 安全风险：当漏洞与安全威胁同时存在时就会存在安全风险
c. 风险管理：风险规避，风险最小化，风险承担，风险转移

9. 信息安全研究内容
a. 基础研究：
i. 密码理论：数据加密算法、消息验证算法、数字签名算法、密钥管理
ii. 安全理论：身份认证、授权和访问控制、审计、安全协议
b. 应用研究：
i. 安全技术：防火墙技术、漏洞扫描和分析、入侵检测、防病毒
ii. 平台安全：物理安全、网络安全、系统安全、数据安全、用户安全和边界安全
c. 信息安全管理研究：
i. 安全策略研究、安全标准研究和安全测评研究

-
- 密码学

1. 密码学（Cryptology）：研究密码系统或通信安全的一门科学。
a. 密码编码学（Cryptography）：寻求保证消息保密性或认证性的方法。
b. 密码分析学（Cryptanalytics）：研究加密消息的破译或消息的伪造。

2. 密码系统
a. 明文：要被发送的原文消息
b. 密码算法：由加密和解密的数学算法组成
c. 密文：明文经过加密算法加密之后得到的结果
d. 密钥：在加密和解密过程中使用的一系列比特串

3. 柯克霍夫原则(Kerckhoffs’ Principle)
a. The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
b. 密码系统安全是基于密钥的而不是算法的保密。

4. 密钥使用方式分类
    a. 对称密码体制
        i. 分组密码
        ii. 序列密码/流密码
    b. 非对称密码体制
5. 密码分析：如果能够对密文的分析确定明文或密钥，或者能够根据明文-密文对确定密钥，这个破译过程称为密码分析。
    a. 数学分析：密码分析者针对加解密算法的数学基础和某些密码学特性，通过数学求解的方法来破译密码。
    b. 物理分析：针对加密电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的侧信道信息泄露而对加密设备进行攻击的方法被称为侧信道攻击。
6. 密码分析
    a. 唯密文攻击(ciphertext only attack)
    b. 已知明文攻击(known plaintext attack)
    c. 选择明文攻击(Chosen plaintext attack)
    d. 选择密文攻击(Chosen ciphertext attacks)
7. 密码作用
    a. 保密性：消息的发送者使用密钥对消息进行加密
    b. 完整性：密码可以保证被接收方收到的消息在传输过程中未经任何变动以保护其完整性。
    c. 不可否认性：以向用户提供不可否认性
    d. 可控性：利用密码技术向其他的用户或系统来证明自己的身份
    e. （差一个可用性）